Plano de Continuidade de Negócios de TI

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Equipe Técnica

Cláudio Rafael Bifi - **Diretor Executivo**

Domingos Sávio Mota – **Diretor de Tecnologia e Infraestrutura**

Ronaldo César da Silva - **Gerente do Departamento de Tecnologia da Informação**

Cláudio Molina Paes Rosa – **Coordenador de Sistemas do Departamento de Tecnologia da Informação**

Alessandro de Melo Beserra – **Coordenador de Redes e Segurança do Departamento de Tecnologia da Informação**

Plano de Continuidade de Negócios de TI

(Versão 3.0)

REVISÕES		
DATA	AUTOR	VERSÃO
19/08/2016	Claudio Molina Paes Rosa	1.0
01/03/2018	Ronaldo Cesar da Silva	2.0
19/10/2021	Claudio Molina Paes Rosa	3.0

Sumário

1. Introdução

O Plano de Continuidade de Negócios de Tecnologia da Informação (PCNTI) contém medidas preventivas, procedimentos de recuperação em eventuais interrupções de negócios, além de assegurar a identificação, avaliação, monitoramento e controle dos recursos que dão suporte à realização das operações (equipamentos, sistemas de informações, pessoal, instalações e informações).

O PCNTI abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI do CRCSP e serviços essenciais, de acordo com o Decreto-Lei n.º 9.295/46 e alterações, para o registro, a fiscalização do exercício da profissão contábil, a normatização e a educação profissional continuada.

O PCNTI é executado tanto no âmbito do TI quanto isoladamente, ou como parte de um Plano de Continuidade de Negócios (PCN) do CRCSP.

Os sistemas gerenciados pelo CRCSP, assim como os recursos que estão dentro da infraestrutura de tecnologia da informação, são serviços essenciais à ativa do CRCSP.

A infraestrutura de tecnologia da informação se encontra na própria sede do CRCSP, se baseando na estrutura com todos os serviços básicos de infraestrutura, como instalações elétricas adequadas, com gerador e no-breaks, ar-condicionado, links de comunicação e equipamentos de conectividade.

Um dos pilares do plano de continuidade de do CRC SP é o procedimento do TI 002, que trata do Backup Geral da Rede, sobre os procedimentos de backup e restore, e os testes que são executados.

1. Objetivos

O PCNTI foi elaborado para atingir os seguintes objetivos:

a) Assegurar integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;

b) Obter capacidade de gerenciar uma interrupção no negócio de forma a evitar impactos para o registro, a fiscalização do exercício da profissão contábil, a normalização e a educação profissional continuada, a fim de proteger a reputação da organização;

c) Manter os sistemas e infraestruturas tecnológicas consideradas essenciais disponíveis;

d) Melhorar proativamente a resiliência da organização em momentos necessários, mitigar os riscos de interrupções e diminuindo o tempo de resposta a possíveis incidentes; e

e) Assegurar através de método sistemático o retorno de operacionalização, em um tempo aceitável dos serviços críticos, após um incidente.

2. Sistemas Essenciais

Os sistemas na tabela abaixo por ordem de prioridade são considerados essenciais para o acionamento e execução do PCNTI:

Sistema	Criticidade	RPO[1]	RTO[2]	Impacto			
				Financeiro	Legal	Imagem	Operacional
Serviços Online	Alta	24 horas	6 horas	Alto	Alto	Alto	Alto
Sistema de Gestão Protheus (TOTVS)	Alta	24 horas	6 horas	Médio	Alto	Alto	Alto
Portal Institucional (crcsp.org.br)	Alta	24 horas	6 horas	Alto	Médio	Alto	Médio
SPI (desktop)	Alta	24 horas	6 horas	Alto	Médio	Alto	Médio
CRC SP Mobile (App)	Média	48 horas	16 horas	Médio	Baixo	Alto	Médio
CRC SP Flow (Intranet)	Média	48 horas	16 horas	Baixo	Baixo	Médio	Médio

[1] RPO: ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura

[2] RTO: período dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

3. Infraestruturas Tecnológicas

Além dos sistemas descritos anteriormente, existem os ativos referentes às infraestruturas físicas, nos quais também são considerados serviços essenciais.

Ativo	Criticidade	Prioridade	Impacto			
			Financeiro	Legal	Imagem	Operacional
Rede de Dados Interna (LAN)	Alta	Alta	Alto	Baixo	Alto	Alto
Link de Dados (WAN)	Alta	Alta	Alto	Baixo	Alto	Alto
Servidor Telefonia	Alta	Alta	Alto	Baixo	Alto	Alto
Energia Elétrica	Alta	Alta	Alto	Médio	Alto	Alto

4. Desastres e Catástrofes Naturais ou Não

Em casos de incidentes, tais como incêndio, não acesso ou outros desastres naturais ou acidentais, após as ações iniciais para contenção dos incidentes, o Comitê de Tecnologia da Informação (CTI) deverá se reunir para identificar os danos causados e assim definir se o PCNTI será acionado.

Serão emitidos relatórios aos Gestores para conhecimento e adoção de medidas julgadas necessárias.

5. Invocação do Plano

O Plano de Continuidade será acionado quando ocorrer algum dos cenários de desastres, insurgência ou ocorrência de um risco desconhecido, e ainda se houver uma vulnerabilidade que tenha grande possibilidade de ser explorada. Poderá invocar o PCTI em casos de testes, ou por determinação do Comitê de TI juntamente com a alta administração do CRC SP.

Os planos de continuidade serão encaminhados para aprovação da Alta Gestão e pelo responsável da Infraestrutura de TI, inseridos os incidentes de interrupção. Interação com áreas provedoras de recursos para operacionalização (TI, Comunicação Social, entre outras).

Os integrantes das equipes, após acionados, iniciarão a avaliação e investigação do ocorrido, podendo acionar outras equipes, caso necessário.

6. Tabela de Responsáveis

Abaixo, segue os contatos dos responsáveis pelas ações a serem tomadas em caso de ocorrência de desastres:

Cargo/ Empresa	Nome	Telefone / Celular

7. Principais Riscos

O PCNTI foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam riscos à continuidade dos serviços essenciais.

O quadro a seguir define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

EVENTO DE DESASTRE	POSSÍVEIS CAUSAS
01- Interrupção de energia elétrica	- Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 24 (vinte e quatro) horas; - Causada por fator interno que comprometa a rede elétrica do prédio com curtos-circuitos, incêndio e infiltrações; - Impossibilidade de acionar o Grupo gerador no momento de uma queda de energia.
02 - Falha na Climatização do CPD	- Superaquecimento dos ativos devido à falha no dimensionamento de carga; - Falha na unidade de climatização e não emissão de alertas de monitoração.
03 - Indisponibilidade de Backup	- Cópia de segurança dos dados não disponível ou sem integridade.
04 - Indisponibilidade de rede/circuitos	- Rompimento de fibra ótica decorrente de execução de obras públicas, desastres ou acidentes; - Mal funcionamento de *switch* gerenciador de segmento de rede; - Interrupção dos serviços de conectividade com as operadoras de telecomunicação por mais de 12 (doze) horas.
05 - Falha humana	- Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível.
06 - Ataques internos	- Ataque aos ativos do *Data Center e à rede CRCSP*.
07 - Incêndio	- Falhas nos equipamentos ou por ação humana.
08 - Falha de hardware	- Falha que necessite reposição de hardware crítico ou reparo, e cujo reparo ou aquisição dependa de processo licitatório.
09 - Ataque cibernético	- Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais, assim como a indisponibilização dos dados por meio de deleção ou mesmo sequestro virtual.

8. Planos de Contingência para Incidentes

Na sequência são apresentados os planos de ação, divididos por ativo da empresa considerados essenciais com risco de falhas de impacto:

Ativo: Serviços Online

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção das atividades finalísticas

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	6 horas	Implantar ação imediatamente
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	6 horas	Implantar ação imediatamente

Ativo: Sistema de Gestão Protheus (TOTVS)

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha do Sistema.	Impacto nos Processo que utilizam o Sistema.	Atualização de versão com falha.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer o sistema de forma funcional.	Assistente de Suporte Técnico.	6 horas	Implantar ação imediatamente.
Reestabelecer a funcionalidade física do servidor (componentes eletrônicos)	Administrador de Rede.	6 horas	Implantar ação imediatamente.
Reestabelecer a funcionalidade do banco de dados do servidor (base de dados).	Coordenador TI.	6 horas	Implantar ação imediatamente.
Viabilizar provisionamento para substituição do equipamento em caso de falha e/ou criação de ambiente redundante.	Diretor TI, Gerente TI, Coordenador TI e Administrador de rede.	6 horas	Implantar ação imediatamente.

Ativo: Portal Institucional (crcsp.org.br)

AMEAÇAS	VULNERABILIDADE	RISCOS
Portal Institucional indisponível	Falhas de DNS ou interrupção do serviço de hospedagem	Perda de acesso dos profissionais e da sociedade ao portal

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Checagem da infraestrutura de rede	Administrador de Rede	6 horas	Implantar ação imediatamente.
Abrir chamado na empresa de hospedagem	Administrador de Rede.	6 horas	Implantar ação imediatamente.

Ativo: SPI (Desktop)

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção das atividades finalísticas

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	6 horas	Implantar ação imediatamente
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	6 horas	Implantar ação imediatamente

Ativo: CRC SP Mobile (App)

AMEAÇAS	VULNERABILIDADE	RISCOS
Acesso indisponível ou funcionamento de forma inesperada (bug).	Erros de programação ou problemas físicos	Interrupção dos recursos do aplicativo para os profissionais

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Solicitar à equipe de desenvolvimento uma análise e correção do problema.	Coordenador de Sistemas	16 horas	Implantar ação em médio prazo
Solicitar à equipe de rede/suporte uma análise quanto à infraestrutura	Coordenador de Sistemas	16 horas	Implantar ação em médio prazo

Ativo: CRC SP Flow (Intranet)

AMEAÇAS	VULNERABILIDADE	RISCOS
Interrupção do Serviço de Intranet, falha no servidor responsável por suportar o serviço intranet.	Fornecimento de acesso ao serviço intranet interrompido.	Perda de acesso os serviços disponibilizados na intranet

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Efetuar o procedimento corretivo utilizando-se de backup para restauração mais relevante do ambiente intranet	Coordenador de TI e Assistente de Suporte Técnico	16 horas	Implantar ação em médio prazo.
Contatar empresa TOTVS que dá suporte ao serviço.	Coordenador de TI e Assistente de Suporte Técnico	16 horas	Implantar ação em médio prazo.

Ativo: Rede de Dados Interna (LAN)

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha no equipamento (switch).	Fornecimento de acesso à rede de forma interrompida, por inexistência de redundância.	Parada da rede Corporativa –LAN.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados interna (LAN).	Administrador de Rede.	Interrupção não tolerável.	Implantar ação imediatamente.
Viabilizar a disponibilização da rede em modo redundante.	Gerente de TI, Administrador de Rede.		Implantar ação em médio prazo.

Ativo: Link de Dados (WAN) - Internet

AMEAÇAS	VULNERABILIDADE	RISCOS
Interrupção do Serviço de fornecimento de acesso internet (WAN) pelo prestador do serviço e falha no equipamento.	Fornecimento de acesso à internet de forma interrompida.	Perda de acesso à internet com indisponibilidade dos serviços de e-mail, WEB e com possibilidade de perdas de transações eletrônicas.

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Reestabelecer de forma emergencial a funcionalidade da rede de dados WAN.	Administrador de Rede.	Interrupção não tolerável	Implantar ação imediatamente.
Viabilizar o fornecimento de acesso em modo redundante para disponibilizar o acesso a internet e seus serviços de forma ininterrupta.	Gerente de TI e Administrador de Rede.		

Ativo: Servidor Telefonia

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha nos equipamentos.	Fornecimento de serviço de voz interrompido por falha adversa, sem aviso prévio e por inexistência de redundância.	Perder a comunicação via telefone com as entidades externas à empresa (CFC, outros CRC´S, delegacias, conselheiros, profissionais da contabilidade e público em geral).

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Utilizar de forma emergencial os telefones celulares corporativos	Gerente de TI e Administrador de Rede.	Interrupção não tolerável.	Implantar ação imediatamente.
Contatar empresa Betta que dá suporte ao serviço.	Administrador da Rede.	Interrupção não tolerável.	Implantar ação imediatamente.

Ativo: Energia Elétrica

AMEAÇAS	VULNERABILIDADE	RISCOS
Falha na prestação do serviço	Fornecimento de energia interrompida por falta de redundância.	Interromper a operação da empresa

AÇÕES	RESPONSÁVEIS	PRAZO MÁXIMO - INTERRUPÇÃO TOLERÁVEL	PRIORIDADE
Executar medidas para preservação dos equipamentos de TI	Gerente de TI e Administrador de Rede.	4 horas	Implantar ação imediatamente.
Contatar o chefe da manutenção sobre prazos de restabelecimento da energia.	Chefe da Manutenção	4 horas	Implantar ação imediatamente.